NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DETERMINING COMMUNICATION SHORTFALLS FOR HOMELAND DEFENSE

by

Kevin P. Wilson

December 2007

Co-Advisors: James A. Russell
Daniel J. Moran

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 2007	Master's Thesis

4. TITLE AND SUBTITLE Determining Communication Shortfalls for Homeland Defense	5. FUNDING NUMBERS
6. AUTHOR(S) Kevin P. Wilson	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT	12b. DISTRIBUTION CODE
Approved for public release; distribution is unlimited.	

13. ABSTRACT (maximum 200 words)

Communications is a critical enabling capability that is interwoven into every facet of every military operation. Assessing what communication capability is most valuable to the operation is a vital planning process that currently resides in several processes that produce differing outcomes within the DoD. This thesis examines these planning processes, particularly the capability-based approach, assessing which process is optimum for determining communication shortfalls.

An in depth comparison of the Joint Capabilities Integrated Defense System (JCIDS) and USNORTHCOM's Capability Review and Resource Assessment (CRRA) was conducted, examining the respective strengths and weakness of each process. This thesis then recommends an optimized hybrid solution of the CRRA and JCIDS, thus providing an intuitive methodology that can be used to model what communication capabilities are essential to the DoD and its interagency partners.

Ultimately, this model may serve to guide the defense planning process to ensure meaningful collaboration occurs, when crafting a unified DoD and interagency position regarding communications and network-centric capability needs and shortfalls. Particular utility can be applied to fill the gap of interoperable communications solutions between first responders, the military, interagency and Coalition partners, when teaming in a homeland defense scenario.

14. SUBJECT TERMS Communication capabilities and shortfalls for Homeland Defense, Capabilities Based Planning for Homeland Defense, Network-centric Environment capabilities and shortfalls for Homeland Defense, C4 (Command, Control Communications, and Computers), Planning for Homeland Defense, Defense Planning and Programming for Homeland Defense, and National Military Strategy for Homeland Defense.	15. NUMBER OF PAGES 75
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DETERMINING COMMUNICATION SHORTFALLS FOR HOMELAND DEFENSE

Kevin P. Wilson
Major, United States Air Force
B.S., South Dakota State University, 1991
M.S., Embry-Riddle Aeronautical University, 1998

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN NATIONAL SECURITY AFFAIRS

from the

NAVAL POSTGRADUATE SCHOOL
December 2007

Author: Kevin P. Wilson

Approved by: James A. Russell
Co-Advisor

Daniel J. Moran
Co-Advisor

Douglas Porch
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Communications is a critical enabling capability that is interwoven into every facet of every military operation. Assessing what communication capability is most valuable to the operation is a vital planning requirement [to avoid using the word process twice in the same sentence] that currently resides in several processes that produce differing outcomes within the DoD. This thesis examines these planning processes, particularly the capability-based approach, assessing which process is optimum for determining communication shortfalls.

An in-depth comparison of the Joint Capabilities Integrated Defense System (JCIDS) and USNORTHCOM's Capability Review and Resource Assessment (CRRA) was conducted, examining the respective strengths and weakness of each process. This thesis then recommends an optimized hybrid solution of the CRRA and JCIDS, thus providing an intuitive methodology that can be used to model what communication capabilities are essential to the DoD and its interagency partners.

Ultimately, this model may serve to guide the defense planning process to ensure meaningful collaboration occurs, when crafting a unified DoD and interagency position regarding communications and network-centric capability needs and shortfalls. Particular utility can be applied to fill the gap of interoperable communications solutions between first responders, the military, interagency and coalition partners, when teaming in a homeland defense scenario.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I wish to thank the following individuals for their support and assistance during the work of this thesis: First, to my beautiful wife, Karen, who inspired and encouraged me through the long hours of research. She has been an incredible sounding board as to the importance and relevance of this topic. Second, to my advisors, Professors James Russell and Daniel Moran, who took time from their hectic schedules to guide me in applying the academic rigor needed to transform my thoughts and passions into a work that is suited for an intellectual body. Third, to Colonel D. J. Johnson and Lieutenant Colonel Mike Connelly, my former bosses from the Air Force Space and C4ISR CONOPS Division at the Pentagon. They both allowed me license to create and to think out of the box. Their support and feedback facilitated the genesis of the hybrid methodology recommended in this thesis to optimize current capability-based planning processes for Homeland Defense. Fourth, to all the action officers at the Pentagon and at USNORTHCOM, who shared with me their frank insight concerning current defense planning processes. Last, but not least, to the U.S. Air Force which for the past 24 years, has trained and educated me in the profession of arms. I will always be grateful to the Air Force; the only institution willing to take a risk on a poor, uneducated, but ambitious boy from the Ozarks of Missouri and provide him with the opportunity to study, grow, and travel the world.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THESIS ARGUMENT

A major shift is occurring within the DoD regarding the development and funding of communication requirements for the services. Transformation from the Cold War, coupled with the events of 9/11, have forced the DoD to change its rules of engagement when it prioritizes and funds communications systems for the warfighter. Aging platforms and the war in Iraq have further increased competition for funding among the services, thus complicating the decision-making process for senior military leaders.

During the height of the Cold War, when pockets were deep and the adversary was a symmetrical actor, funding decisions were reached using the BOGSAT[1] (Bunch of Guys Sitting at the Table) method. This method was an exercise in service parochialism steeped in emotion and politics, where the highest ranking or most protected leader prevailed. Over time, the BOGSAT system evolved into a more qualitative approach, where requirements were validated by linking mission impact to the perspective communication system. However, this approach still lacked the quantitative rigor necessary to ascertain an objective analysis.

In June of 2003, the DoD issued CJCSI 3170.01, Joint Capabilities Integration and Development System (JSIDS), with the intent to migrate from a platform-centric procurement process to a capability-centric approach[2]. This approach employs a series of Joint Functional Concepts (JFCs) to identify critical capabilities that deliver a desired effect to the combatant commander. In the communications arena, the Network-Centric Environment (NCE) JFC is utilized to capture communication shortfalls for the DoD. The Air Force[3] in and Navy[4] has since followed suit, by developing their own service-centric Capability-Based Planning (CBP) process to identify communication shortfalls.

---

[1] Ernest Forman, Decision by Objectives: How to Convince Others that you are Right, http://mdm.gwu.edu/forman/DBO.pdf, 6 (August 2007).

[2] Chairman of the Joint Chief of Staff Instruction 3170.01, Joint Capabilities Integration and Development System (2003), 1.

[3] U. S. Air Force Instruction 10-604, *Capability Based Planning* (2006), 3.

[4] U. S. Navy FORCEnet, What is the Value- Added of FORCEnet, forcenet.navy.mil/fn-definition.htm (19 November 2006).

This thesis examines current methodologies used in the DoD to ascertain communication and network-centric capability shortfalls for warfighters and first responders. The objective is to develop an intuitive and meaningful methodology that defense planners and programmers can adopt to discern communication shortfalls, quantify and articulate those shortfalls, and then, in turn, use that data to help decision makers prioritize funds when procuring systems that provide communication capabilities for Homeland Defense.

B. RESEARCH QUESTION

The key research question analyzed is: Does CBP possess the right methodology to assist defense planners and programmers in determining capability gaps/shortfalls? The following sub-questions provide further granularity and analysis of the research problem:

- How can the CBP process be more intuitive?
- How does CBP determine capability gaps?
- How does the output of CBP provide meaningful data for decision makers to prioritize procurement funds? What is this data?
- How can CBP be improved to better determine communication shortfalls?

Little is published regarding CBP. This is a new discipline within the DoD that is gaining momentum, but is not well documented. Two sectors studied provide the framework of existing knowledge for CBP: Needs Determination Planning in the corporate sector and the Joint Capabilities Integration and Development System for the DoD.[5]

Though the Needs Determination Planning process provides utility in the corporate world, it is nearly identical to the traditional procurement process used for

[5] Thus far, a significant amount of work has been done within the Air Force as a stand-alone service, namely the Capability Risk and Review Assessment (CRRA). Unfortunately, the Air Force has not yet bridged the gap that exists as a component to the Combatant Commander (COCOM) concerning communications or Network-Centric Environment CBP methodology. Considering this, the focus of this thesis will be to develop the correct methodology the defense planner and programmers can use to gather shortfalls for the COCOM, more precisely, USNORTHCOM, with respect to Homeland Defense and First-Responder support.

years by the services. This process involved units submitting their requirements to their respective headquarters, after which panels were formed to rack and stack these requirements.[6] Then, the board or panels would ultimately decide or not decide to fund them. Years of executing this process often revealed that a less than optimum solution was procured and left the operator lacking the needed capability to accomplish the mission. This occurred because capability effectiveness was not measured or evaluated. Systems or platforms were procured based on requirement documents without any evaluation of capability analysis performed.[7]

In relation to the DoD sector, available literature includes DoD instructions and Joint Functional Concepts. There is no text book to assist planners on the art of CBP methodology or processes. The DoD instruction describes a capability assessment used by Combatant Commands, known as Joint Capabilities Integration and Development System. Currently, several methodologies exist in the DoD and each one differs in their application and execution. Each directorate of the Joint Staff employs its own unique Joint Functional Concept. Nearly every concept discusses communications, but each concept differs in articulating and quantifying what a capability is and how to measure its effectiveness.[8]

Existing literature falls short of addressing the NORTHCOM problem of planning and funding communication capabilities for Homeland Defense. Exhaustive research revealed that no literature exists in the corporate sector that addresses CBP. Current literature regarding the corporate sector pertains to strategic planning, but does not address a capabilities based approach. The DoD instruction provides over-arching

[6] The corporate sector does not use CBP per se. However, according to Dr. Ron Schill, MBA Professor at the Monterey Institute of International Studies, a method known as Need Determination Planning is used in industry, which is akin to CBP, incorporating similar processes. Ron Schill, Ph. D, is a visiting Professor, Fisher Graduate School of International Business, Monterey Institute of International Studies. He is a professor emeritus from the Marriot School of Business at Brigham Young University, with over 30 years of teaching and research devoted to strategic planning and marketing. Interviewed by Kevin Wilson. (2006).

7 U. S. Air Force Instruction 10-604.

[8] Mike Connelly, Lieutenant Colonel, Deputy Director, Space and C4ISR Concept of Operations, AF/A5XC-SC, Pentagon, Washington, DC. Interview by Kevin Wilson. (2006). See also, Chairman of the Joint Chiefs of Staff Joint Functional Concept. Battle Space Awareness. Washington DC. 2003, Chairman of the Joint Chiefs of Staff Joint Functional Concept. Joint Command and Control. Washington DC. 2005, and Chairman of the Joint Chiefs of Staff Joint Functional Concept. Net-Centric Environment. Washington DC. 2005.

guidance of the capability planning process, but lacks specified direction to ascertain communication capability shortfalls. The JFC provides a very technical approach to discern capability shortfalls, but does not address specific capabilities for war fighters or first responders working in a collaborative environment in an inter-agency, federal, state, or local setting.[9]

This research originated from mainly primary sources, as secondary sources are scarce. The primary sources consist of raw data and methodology developed at the Pentagon, coupled with interviews from DoD subject matter experts.

The study of this problem will involve a careful review and re-evaluation of existing DoD and Air Force CBP processes. It will also entail primary source interviews of Pentagon and NORTHCOM planners with the possibility of onsite visits for test scoring purposes. This feedback and mock data will enable the development of a new process to find existing communication and network-centric capability gaps for warfighters and first responders working in a collaborative environment.

C. APPLICABILITY

This research is intended to provide alternative methods for Combatant Commands, primarily USNORTHCOM, to plan and fund communication capabilities for Homeland Defense. US Joint Forces Command may also find value in this process and use it as a template across the DoD and Joint Staff.

Further, this thesis will stress the importance of collaboration among the COCOM, Joint Staff, and services when planning, staffing and executing the Program Objective Memorandum (POM) during and between Future Years Defense Program (FYDP).

[9] Mike Connelly, Lieutenant Colonel, Deputy Director, Space and C4ISR Concept of Operations, AF/A5XC-SC, Pentagon, Washington, DC. Interview by Kevin Wilson. (2006). See also, Chairman of the Joint Chiefs of Staff Joint Functional Concept. Battle Space Awareness. Washington DC. 2003, Chairman of the Joint Chiefs of Staff Joint Functional Concept. Joint Command and Control. Washington DC. 2005, and Chairman of the Joint Chiefs of Staff Joint Functional Concept. Net-Centric Environment. Washington DC. 2005.

This is a critical element of defense planning since precious resources are often wasted as the result of poor collaboration and non-standard processes occurring simultaneously which fail to capture a unified DoD position when articulating capability needs and shortfalls.

THIS PAGE INTENTIONALLY LEFT BLANK

II. COMMUNICATION SHORTFALLS: BACKGROUND AND FRAMEWORK

A. WHAT CONSTITUTES COMMUNICATIONS?

The world is now at the height of an information revolution where the dissemination and analysis of data is critical to government, commerce, and world culture. From a national defense perspective, communications is an enabling capability that is interwoven into every facet of military operations. The term "communications" is often interchanged with concepts such as: the Network-Centric Environment and C4 (Command, Control, Communications, and Computers).[10] This is mainly due to the evolvement of electronic technology with the advancement of electrical component miniaturization, as well as that of computers, computer software, and its internet-worked architectures.

During World War II and through the Cold War, the term communications represented a category of technology such as: radio, radar, telephone, telegraph, and teletype. By the 1960's satellite communications were introduced to the DoD[11], which provided an optimized voice or telephony[12] capability to the warfighter, and ushered in space-based communication technology.

An important step occurred in 1969, when the University of California at Los Angeles installed the first Advanced Research Projects Agency node[13], sharing digital packet information with the Stanford Research Institute, the University of California at Santa Barbara, and the University of Utah.[14] This birth of the Internet further shaped military communications as it merged traditional communications, such as radio, video,

---

[10] The Joint Chief of Staff, *The National Military Strategy of the United States of America, A Strategy for Today; A Vision for Tomorrow*, 2004, 19, 27.

[11] Committee on Evolution of Untethered Communications, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications National Research Council, *The Evolution of Untethered Communications*, National Academy Press: Washington, DC, 1997, 1.2.5.

[12] The JCS Glossary of Communications-Electronics Terms defines telephony/voice as: A form of telecommunication primarily intended for the exchange of information in the form of speech.

[13] Ibid: A point of interconnection to a network; One of the switches forming the network's backbone.

[14] *The Evolution of Untethered Communication*, 1.2.7.

and telephony services, with computer technology. This synergy became known as network-centric, as these services can now be integrated and transported over networks and shared with multiple users.

The Network-Centric Environment is defined as: "a framework for full human and technical connectivity and interoperability that allows all DoD users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence, and protects information from those who should not have it."[15]

Several of these terms require further definition. First, the concept technical connectivity implies equipment or hardware that is connected or interconnected together. Second, interoperability can be defined as: "The ability of systems, units or forces to provide services to and accept services from other systems, units or forces and to use the services so exchanged to enable them to operate effectively together."[16] Third, information is: "Facts, data, or instructions in any medium or form with context that is comprehensible to the user."[17] Finally, "all DoD users and mission partners" refer to all branches of the services working with interagency partners, such as the intelligence community, the Department of Homeland Defense, the State Department, the Department of Justice, and etc. Needless to say, many of the challenges in the communications area, from ad DoD perspective, arise from the dramatic recent expansion of who its "mission partners" might be under given circumstances, and the need to develop systems that can take account of their requirements in a timely manner.

Simply put, communications, C4, the network-centric environment, or net-centricity, might be best understood in the context of homeland defense as: Connectivity and interoperability that allows all DOD users and mission partners to include: Joint,

---

[15] The Department of Defense, Joint Functional Concept, *Network-centric Environment*, 7 April 2005, 1.

[16] The Combined Communications-Electronics Board, Glossary of Communications-Electronics Terms, ACP 167(I), March 2005, 2-88

[17] Joint Functional Concept, *Network-Centric Environment.* B-2.

Coalition, and Inter-Agency users to share information when they need it, in a form they can understand and act on with confidence, and which also protects information from those who should not have it.

Now that a working definition of communications has been established, it is important to examine the components, or functions, that make up the repository of communications or net-centricity. Three categories provide a valuable framework for this discussion.[18] They are: voice, video, and data. The following definitions depict these categories:

- Voice - Provide information via [human or computerized] voice to include: radio, phone, interphone, voice-over IP, or public address system.[19] Or, the frequency of an acoustic oscillation which may be produced by the normal human voice.[20] For further clarity, interphone is defined as: A telephone apparatus by means of which personnel can talk to each other within an aircraft, tank, ship or activity.[21] Voice systems are typically found in radios that reside in aircraft, ships, ground vehicles, and portable backpacks versions.
- Video - Information such as: streaming video, video teleconferencing, live transmissions, or recorded video.[22] Video is the images captured by camera and displayed via various types of displays such as: a computer, television, cell phone, multi-function displays in aircraft, ships, our ground vehicles. In a collaborative setting, video is captured via a web camera or cellular phone and shared over the internet or cellular network as raw data or during chat sessions.
- Data - Text or imagery such as: digitized photos, forms/publications, email, messages, web pages, chat sessions, or audio files.[23] This data is created by manual input such as a keyboard, stylus, digital camera, or scanner. The data is disseminated manually by humans or automatically by machine, network, or internet processes.

[18] U.S. Air Force, *Master Capabilities Library, Net-Centricity*, version 6.0, 2007.

[19] Ibid.

[20] ACP(I) 167, 2-171.

[21] Ibid., 2-88.

[22] Master Capabilities Library, Net-Centricity.

[23] Ibid.

B. HOW ARE COMMUNICATIONS APPLIED TO HOMELAND DEFENSE?

As Section A defined the basics of communication capabilities, this section will depict how basic capabilities are used in a homeland defense environment. Communications applied to the defense arena, specifically applied to homeland defense, become more complex and advanced. In addition to enabling C4 functions, communications enable space, intelligence, surveillance, and reconnaissance (ISR) functions.[24] Space and C4ISR platforms are extremely network-centric. They are a system of systems interconnected via networks to collect, process, and disseminate data. Further, Space and C4ISR platforms typically integrate the three categories of communication capability defined in section A, namely: voice, video, and data. For example, a Defense System Communication Satellite III is capable of sending voice, video, and data worldwide to a variety of military and government users. The satellite itself orbits in space at an altitude of 22,000 miles, but is controlled by a series of ground stations that are interconnected by network-centric technology. Users on the ground, at sea, or in air can access this system to receive and disseminate data to conduct operations.[25]

In addition to disseminating data, imagery and infrared sensors reside on defense satellites providing valuable ISR for homeland defense. Infrared sensors on the Defense Support Program Satellite, provides early warning detection of missile launches against the United States or personnel operating overseas. Again, this is a high orbiting satellite that is controlled by ground stations that are interconnected by network-centric capability and the information is processed, analyzed, and disseminated by similar technology.[26]

The next important facet of these capabilities is the integration of these various sensors, signals, and raw data. What is critical for the DoD and its interagency partners is the sharing of these systems to make intelligible decisions. This is often called decision-quality information derived from sensor integration or decision superiority.[27] The newly

---

[24] Department of Defense, *Strategy for Homeland Defense and Civil Support*, June 2005, 3.

[25] U.S. Air Force Fact Sheet, *Defense System Communication Satellite*. http://www.af.mil/factsheets/factsheet_print.asp?fsID=95&page=1, (Accessed 5 April 2007).

[26] Ibid. http://www.af.mil/factsheets/factsheet.asp?id=96, (Accessed 5 April 2007).

[27] Joint Functional Concepts, *Battle Space Awareness*, 15 and *Net-Centric Environment*, 6.

published Joint Operating Concept for Homeland Defense and Civil Support provides an excellent explanation of this concept, discussed in the Battlespace Awareness section of the document: "Battlespace awareness is the ability of the Joint Force Commander to understand the operational environment, the full array of interagency and international capabilities, and the adversary. To ensure DOD can detect, deter, prevent, or if necessary defeat threats to the Homeland and assist in mitigating the effects of attacks that do occur, the Joint Force Commander must have a comprehensive understanding of the battlespace (within the limits set by law). This includes the capability to detect the full range of threats enabled through an interlocking field of sensors with deep reach and remote surveillance capability, fused with national-level intelligence collection and analysis to provide common situational awareness across the spectrum of participants for all domains in the operating environment (air, space, land, maritime, and cyber). For HD and CS, this includes shared awareness (including non-intelligence sources) between numerous government and non-government participants."[28]

In addition to the interlocking or integrating a field of sensors and the fusing of national level intelligence discussed here, an underpinning of information sharing is essential to decision or information superiority. This implies technical solutions, as well as a profound alteration of the culture of sharing information that has traditionally existed within the intelligence community, the DoD, and its likely coalition or interagency partners. This is perhaps the most difficult barrier to overcome since it involves the human element of how operations are conducted. This can be overcome by fostering a spirit of openness and sharing. This concept is described in the net-centric JFC as end-to-end transparency. This is a concept of opening up technical and cultural barriers, thus providing information to those who need it and is defined as: visible, accessible, understandable, verifiable, current, and trusted.[29]

A final important communication concept applied to homeland defense is the advent of wireless technology. Wireless solutions provide homeland defense personnel with portable, lightweight, and secure capability which allows for the collection, analysis,

[28] Chairman of the Joint Chiefs of Staff Joint Operating Concept, *Homeland Defense and Civil Support*, Washington DC, September 2006, 51.

[29] Joint functional Concept, *Net-Centric Environment*, 16.

and dissemination of information.[30] This is an important aspect since these personnel may deploy, in an austere or a ravaged environment where fixed infrastructure is not available or has been damaged by an attack or natural disaster. This technology provides an agility factor for personnel who must deploy with little or short notice and have limited space and weight allowances to transport large amounts of equipment and personnel to operate it.

A few of these devices may include: personal digital assistants, cellular telephones, laptop or knee board computers, hand held radios, global positioning service receivers, and a myriad of wireless sensors to collect and disseminate vital imagery, weather, and chemical, biological, radiological, nuclear, and explosive (CBRNE) data.

Wireless technology provides interconnectivity from the sensor to the decider to the shooter and or responder. It provides a push pull collaborative ability between these entities, facilitating centralized decision making with decentralized execution. An effective wireless solution has the ability to integrate the three components of communications, voice, video, and data, in a seamless manner to those individuals who require and are authorized access to the information.

An area of technology that is bringing wireless technology to fruition is the development and fielding of unmanned aerial vehicles (UAVs). UAVs are able to collect various ISR information, such as: voice, video, data, weather, radar, and CBRNE, and disseminate it back to distribute ground systems for processing and analysis. This information can then be pushed or pulled to various personnel who may need it to conduct homeland defense missions in virtually any environment, in the air, on land or sea, or from space.

C. WHAT IS A SHORTFALL AND WHY IS IT IMPORTANT?

Before shortfalls can be discussed, it is essential to understand what a capability is. Capabilities are often confused with systems, platforms, tasks, or effects. The joint staff defines capability as: "The ability to execute a specified course of action. It is defined by an operational user and expressed in broad operational terms in the format of

[30] Defense Information Agency, *FY 2004/2005 Budget Estimate*, Research, Development, Test, and Engineering Budget Item Justifications, February 2003.

an initial capabilities document or a DOTMLPF change recommendation. In the case of material proposals, the definition will progressively evolve to DOTMLPF performance attributes identified in the CDD and the CPD."[31]

Though a system or platform delivers capability and provides effects, it is not a capability in itself. Computer networks and handheld radios are systems or solutions, not capabilities. They provide capabilities such as, wireless voice and data services to the operator, but are not capabilities by themselves.

Nor should capabilities be confused with tasks. Regarding communications and NCE capabilities, the capability may be: provide voice communications on the ground, air, or sea, and not install VHF radios, antennas, and cabling in ground facilities. The capability is the what, not the how or why. Capabilities are produced by systems and platforms and contribute the desired effect, but are not stand-alone systems, platforms, or effects.

As capability has been defined, shortfalls and gaps must be understood. In the capabilities planning arena, gaps and shortfalls are used interchangeably. The joint community explains capability gap(s) as: "The capabilities are identified by analyzing what is required across all functional areas to accomplish the mission. The gaps or redundancies are then identified by comparing the capability needs to the capabilities provided by existing or planned systems."[32] The inability to provide those needs results in a capability gap or shortfall.

This often tedious process requires that available integrated architectures be analyzed and compared to the combatant commands Integrated Priority Listing. The IPL is the operational requirement stated by the combatant command and is often non-descriptive. The challenge is matching these non-descriptive requirements to existing or future systems that may or not provide the needed capability. Another challenge to be mindful of is that integrated architectures are not systems, but: "An architecture

[31] Chairman of the Joint Chief of Staff Instruction 3170.01, *Joint Capabilities Integration and Development System* (2003), GL-4. DOTMLPF is defined as: doctrine, organization, training, materiel, leadership and education, personnel, and facilities; CDD is defined as: capability development document; and CPD is defined as: capability production document.

[32] Chairman of the Joint Chief of Staff Manual 3170.01B, *Operation of the Joint Capabilities Integration and Development System* (11 May 2005), GL-10.

consisting of multiple views or perspectives (operational view, systems view and technical standards view) that facilitates integration and promotes interoperability across capabilities and among related integrated architectures."[33] What planners must do during this process is to establish the linkages between architectures and systems.

In the context of NCE, information support plans aid the process by establishing these linkages by describing: "system dependencies and interface requirements in sufficient detail to enable testing and verification of information technology (IT) and National Security Systems (NSS) interoperability and supportability requirements. The ISP shall also include IT and NSS systems interface descriptions, infrastructure and support requirements, standards profiles, measures of performance and interoperability shortfalls."[34] This is important, because NCE is an enabling capability that underpins all military operations. Therefore, system dependencies, interface requirements, and interoperability must be in constant consideration.

What is the importance of communication gap analysis? Aside from merely heightening everyone's awareness that communications are the enabling capability of most military/civil operations, its real utility comes from how it affects the decision maker who allocates funds. The catch phrase often heard at the Pentagon by senior officers and executives is: "If I had one more dollar to spend, where should it go?" Gap analysis helps answer this question by inserting several decision points into the acquisition process that forces the decision maker to assess how capability gaps are maturing and where to direct resources to close these gaps. If the maturity process is going poorly, flag officers and senior executive may decide to stop funding to a particular program and divert funds where more progress is being made.

If the shortfall is validated correctly, in the context of meticulous capability-based planning, a common thread or traceability may be established throughout a myriad of operations. For example, if it is determined that a data shortfall has been identified and it

[33] Chairman of the Joint Chief of Staff Manual 3170.01B, *Operation of the Joint Capabilities Integration and Development System*, (11 May 2005), GL-9.

[34] Ibid., GL-8.

is occurring across several joint capability areas[35], such as: land, sea, space, and defense support of civil authority operations, this implies the criticality of this particular shortfall. This provides decision makers an integrated analysis to consider what is more rigorous and objective than traditional procurement processes. This provides combatant commanders' shortfalls to present that have been validated in a joint environment across several types of operations, thus lending to the credibility of the funding decision.

Though some capability-based planning methodology has been discussed here to aid the discussion of communication shortfall/gap analysis, a more thorough discussion is required and will be discussed in subsequent chapters of this thesis.

[35] The Joint Staff provides two definitions for Joint Capability Areas (JCAs): 1. An integral part of the evolving Capabilities-Based Planning process…the beginnings of a common language to discuss and describe capabilities across many related Department activities and processes, (SECDEF Memo, 6 May 2005). 2. JCAs are collections of capabilities grouped to support capability analysis, strategy development, investment decision making, capability portfolio management, and capabilities-based force development and operational planning, (JCA Baseline Reassessment Terms of Reference).

THIS PAGE INTENTIONALLY LEFT BLANK

III. DEFENSE PLANNING PART I: CONNECTING THE DOTS

A. AMERICA'S GRAND STRATEGY

Since the passage of the Goldwater-Nichols Act of 1984, every president has been required to issue an annual statement called the National Security Strategy of the United States of America. These documents represent, by definition, the most senior national defense guidance that exists at any given moment. They are also, by nature, so general in their application, and so broad in scope, that their practical application to real-world defense planning is inevitably open to question.

Planners and programmers of the capabilities-based persuasion in particular are inclined to question the value of attempting to establish concrete linkages between such high-level policy and the process of procuring capabilities, which, once procured, are by nature much less easy to change than whatever strategic language may have inspired their acquisition in the first place. Nevertheless, politics also has its practical realities, no less than the procurement process does, and it is a fact that when budgets leave the Pentagon or Congress, and are awaiting signature at the White House, programs that provide capabilities for homeland defense (or any other military mission) stand a better chance of survival if there is a legitimate linkage to the National Security Strategy.

Therefore, the first step is to identify objectives from this strategy that would require the enabling capability of communications or network-centricity. The March 2006 strategy contains nine objectives to help secure America. Of these nine, seven can be legitimately linked to communications or network-centric capabilities provided by the military. Consequently, the remaining section of this chapter will elaborate on these seven objectives and link the type of communication capabilities that might enable these objectives with respect to homeland defense.

The first objective, Champion Aspirations for Human Dignity, is a rather intangible objective as it speaks to ending tyranny and spreading democracy. However, pertaining to the third element of the "Way Ahead" section of this objective titled: "How We Will Advance Freedom: Principled in Goals and in Pragmatic in Means," a linkage is

found.[36] Here the following tool is discussed: "Tailoring assistance and training of military forces to support civilian control of the military and military respect for human rights in a democratic society."[37] This concept is deeply steeped in homeland defense with regards to civil support provided by the military. It implies a full spectrum of communications capabilities that enable operations occurring in collaborative environments between the military, interagency, federal, state, and local partners such as: natural disasters, humanitarian efforts, or attacks on the homeland.

The second objective of the national security strategy called: "Strengthen Alliance to Defeat Global Terrorism and Work to Prevent Attacks Against Us and Our Friends."[38] This objective calls out two elements tied to communication capabilities. The first element: "Prevent attacks by terrorist networks before they occur", requires a find, fix, target, track, engage, and assess model to disrupt, capture, and or kill terrorists. Communication capabilities which enable this to occur are in the sensor-to-shooter integration and in the collection and dissemination of intelligence, primarily in the human and communications intelligence genre.[39] The second element: "Deny WMD to rogue states and to terrorist allies who would use them without hesitation", involves the collection, analysis, and dissemination of CBRNE weapon proliferation intelligence.[40] Sensor-to-shooter integration, coupled with interoperable network connectivity for homeland defenders and the intelligence community, brings this objective to fruition.

Linkage three is contained in the objective: "Work with Others to Defuse Regional Conflicts."[41] This objective discusses the need for the U.S. to work with coalition and foreign governments for conflict intervention and post conflict stabilization and reconstruction. Interoperable network-centric communications and intelligence sharing is essential to meet the intent of this objective.

---

[36] The White House, *The National Security Strategy of the United States of America*, March 2006, 2-6.

[37] Ibid., 6.

[38] Ibid., 8.

[39] Ibid., 12.

[40] Ibid.

[41] Ibid., 16.

The fourth association is embodied in the requirement to: "Prevent Our Enemies from Threatening Us, Our Allies, and Friends with Weapons of Mass Destruction."[42] This objective is closely related to the second linkage as it utilizes the same communications capabilities for WMD and CBRNE. However, this objective introduces missile defense and pathogen detection. The U.S. Missile Defense System is a space/ground based defensive and offensive system highly reliant on network-centric technology to find, fix, target, track, engage, and assess incoming missiles bound for the homeland. It employs sensor-to-shooter integration and relies on a highly robust and sophisticated command and control structure. This objective also describes new offensive nuclear and conventional strike capabilities, which would require shooter-to-shooter integration and enhanced nuclear command and control capabilities.

Objective five: "Develop Agendas for Cooperative Action with Other Main Centers of Global Power", captures the need for joining with other nations and the transformation of NATO to stabilize international security vulnerabilities.[43] Interoperable network-centric systems, collaborative tools, and intelligence sharing is necessary for this objective to take root.

The sixth objective: "Transform America's National Security Institutions to Meet the Challenges and Opportunities of the 21st Century", is a national security objective which is extremely reliant on automation.[44] Transformation which really equates to over two decades of doing more with less and the constant downsizing of the military necessitates the military to rely on network-centricity and information dominance to enhance operations in the coalition, joint, and interagency environment.

The seventh and final objective that is linked to communication capabilities is: "Engage the Opportunities and Confront the Challenges of Globalization". This addresses public health challenges like pandemics and cataclysmic events which tax first-responder support.[45] Again, intelligence and information sharing, interoperable networks, and wireless technologies enable the accomplishment of this objective.

---

[42] The White House, *The National Security Strategy of the United States of America*, March 2006, 18.

[43] Ibid., 35.

[44] Ibid., 43.

[45] Ibid., 47.

B. AMERICA'S DEFENSE STRATEGY

The National Defense Strategy of the United States of America is the Department of Defense's plan to align its objective against America's grand strategy. Published in March 2005, it was better aligned with the White House's National Security Strategy of September 2002. Nonetheless, similarities reside in the two documents and the Pentagon has made the connection in the strategic objectives, implementation guidelines, and in the desired capabilities and attributes section of the document.

Primarily, America's defense strategy speaks of building on the 2001 Quadrennial Defense Review by implementing transformation via a capabilities approach. Four strategic objectives have been established which link fairly well to the grand strategy. They are: "secure the United States from direct attack; secure strategic access and retain global freedom of action; strengthen alliances and partnerships and establish favorable security conditions." [46] These four objectives would require the same type of enabling communication capability as were linked to America's National Security Strategy, namely voice, video, and data used in the air, land, sea, and space domains. Further, the same attributes would also apply, such as: interoperability and multi-level security. Multi-level security speaks to information sharing amongst mission partners who have a need to know. These partners may exist as: foreign governments/coalition partners; interagency partners; federal, state, local, and tribal governments; and joint military organizations. Though attributes will be discussed in great detail in chapter five of this thesis, it is important to introduce this concept, as this strategy is steeped in a capabilities based approach.

As stated in this strategy: "Capabilities-based planning focuses more on how adversaries may challenge us than on whom those adversaries might be or where we might face them. It focuses the Department on the growing range of capabilities and methods we must possess to contend with an uncertain future. It recognizes the limits of intelligence and the impossibility of predicting complex events with precision. Our planning aims to link capabilities to joint operating concepts across a broad range of

[46] The Department of Defense, the National Defense Strategy of the United States of America, March 2005, iv.

scenarios."[47] It can be argued that this is one of the key elements used to transform the military, shifting focus from a threat-based planning model to the capability-based model.

This document goes on to introduce the Defense Department's desired capabilities and attributes. There are eight of them. They are:[48]

1. Strengthen Intelligence
2. Protecting Critical Bases of Operation
3. Operating from the Global Commons
4. Protecting and Sustaining Forces in Distance Anti-Access Environments
5. Denying Enemies Sanctuary
6. Conducting Network-Centric Operations
7. Improving Proficiency Against Irregular Challenges
8. Increase Capabilities of Partner-International and Domestic

This is where this document begins to unravel. These eight items do not meet the criteria of defined capabilities per the guidance from the Joints Chiefs of Staff. Per their guidance, the J7 has identified and grouped operational capabilities into tiers, thus prioritizing and establishing a common language amongst the joint community. For example, the J7 has a few of the following as core capability areas:[49]

- Joint Land Operations
- Joint Maritime/Littoral Operations
- Joint Air Operations
- Joint Space Operations
- Joint Access & Access Denial Operations
- Joint Information Operations

The difference between the two lists is apparent. The first is a list of objectives or tasks, whereas the latter are distinct capability areas employed by the military. Hence, this is where the confusion begins in the planning and programming communities. It incites the community to lean back towards their comfort zone and think in terms of requirements, task, systems, and platforms.

[47] The Department of Defense, the National Defense Strategy of the United States of America, March 2005, 11.

[48] Ibid., 12-15

[49] The Chairmen of the Joint Chiefs of Staff, *Joint Capability Areas 101*, J7/JETCD, April 2007, 6.

The other document that is responsible for defining national defense strategy is the National Military Strategy of the United States of America. This document is intended to bridge the gap between the White House and the SECDEF strategies. Signed in 2004 by former Chairman of the Joint Chiefs of Staff, General Richard B. Myers, it focuses on capabilities and attributes. They are:[50]

- Applying Force
- Deploying and Sustaining Military Capabilities
- Securing Battlespace
- Achieving Decision Superiority

Like the National Defense Strategy, these four capabilities do not meet the criteria as defined by the J7 as capability areas. Again, these four items are more objectives or tasks. Another problem with the defense strategy is how attributes are defined. In the National Defense Strategy of 2005, two attributes are identified: shape and size of military forces and global defense posture.[51] These are not attributes, because they cannot be measured. However, in the National Military Strategy, the following joint force attributes are listed:[52]

- Fully Integrated
- Expeditionary.
- Networked
- Decentralized
- Adaptable
- Decision superiority
- Lethality

These attributes are more readily measurable, often associated with a unit of measure such as a percentage. Therefore, work remains to refine these documents to establish a common language in the planning community.

---

[50] The Joint Chiefs of Staff, *The National Military Strategy of the United Sates of America, A Strategy for Today; A Vision for Tomorrow*, 2004, 16-19.

[51] The National Defense Strategy of the United States of America, 16-19.

[52] The National Military Strategy of the United States of America, 15.

C. USNORTHCOM'S DEFENSE STRATEGY

The next linkage that requires analysis is how USNORTHCOM implements grand and defense strategy. NORTHCOM's strategy is derived from the 1 December 2006 document titled, Strategic Guidance, Defending Our Homeland. Though this document does not mention America's security, defense, or military strategies, a linkage can be found in the dilation of its strategic goals and objectives. The intent of this document is to: "provide strategic direction to ensure unity of effort within and between NORAD and USNORTHCOM."[53]

NORAD and NORTHCOM are collocated in Building 2 at Peterson Air Force Base in Colorado Springs, Colorado, staffed with over 1,400 Army, Navy, Air Force, Marine Corps, Coast Guard, civilian and Canadian personnel. These two commands have complementary missions to secure the North America. The following mission statements depict these complementary roles:

NORAD Mission Statement

- Detect, validate, characterize, assess and warn of attacks against North America whether by aircraft, missiles or space vehicles. Detect and respond to unauthorized and unwanted air activity approaching or operating within North American airspace. Process, assess and disseminate intelligence/information to warn of maritime threats or attacks against North America. [54]

USNORTHCOM Mission Statement

- Conduct operations to deter, prevent, and defeat threats and aggression aimed at the United States, its territories and interests within the assigned area of responsibility; and as directed by the President or Secretary of Defense, provide defense support of civil authorities including consequence management operations. [55]

[53] NORAD/USNORTHCOM, *Strategic Guidance - Defending Our Homeland*, 1 December 2006, 1.

[54] Ibid., 3

[55] Ibid.

Simply, NORAD's responsibilities remained unchanged prior to 9-11 whereas NORTHCOM was established to handle the interagency and military/civil relations issue.

These complementary roles can be further articulated and the nuances detected in the two commands by the following strategic goals:

NORAD's Strategic Goals[56]

1. Detect, deter, and defend against aerospace threats to North America
2. Provide timely, accurate maritime warning of threats to, and attacks against North America
3. Be a model for international cooperation in defense planning, execution, training, information management and technological innovation

USNORTHCOM's Strategic Goals[57]

1. Detect, deter, prevent, and defeat external threats and aggression
2. Provide timely and effective defense support of civil authorities
3. Improve unity of effort with our interagency and international partners

Combined Strategic Goal

- Create a more agile organization that takes care of its people and meets the challenges of the 21st Century[58]

Though this organization appears redundant, it is solidified by one commander, who is dual-hatted to lead both commands. A similar model to what was used when]USSPACECOM and NORAD were led by one four-star flag officer from the 1980's through 2002. In October 2002, USSPACECOM was disbanded, with the Space and C4ISR roles transferred to USSTRATCOM.

This is not to say that NORAD and USNORTHCOM have relegated all Space and C4ISR oversight to USSTRATCOM. On the contrary, the very nature of securing America via NORAD and NORTHCOM is completely reliant on Space and C4ISR capabilities. In reality, what is occurring is a division of labor to divvy up this

[56] NORAD/USNORTHCOM, *Strategic Guidance - Defending Our Homeland*, 1 December 2006, 5-6.

[57] Ibid., 7-8

[58] Ibid., 9.

tremendous workload associated with planning, programming, and executing the types of capabilities and assets required to support the above strategic objectives.

Further dilation of NORAD's/NORTHCOM strategic guidance is derived from NORTHCOM's Concept of Operation Plan (CONPLAN) 2501-05. This 555 page CONPLAN, published in April 2006, was created to fulfill the following requirement: "USNORTHCOM CONPLAN 2501-05 fulfills a requirement established in the Joint Strategic Capabilities Plan (JSCP) 02 Change 1, Regional Tasking 9. The CDRUSNORTHCOM was directed to prepare a plan to support the employment of DOD forces providing Defense Support of Civil Authorities (DSCA) IAW applicable DOD directives and policy."[59]

This plan was crafted to help bridge the gap from strategic guidance to actionable tasks of securing the homeland. It contains 10 annexes which call out specific actions to meet the commander's intent. Of the 10 annexes, seven invoke communications or NCE capabilities. The following table links some of the more critical communication/NCE capabilities to the applicable annex:

Annex	**Communications/NCE Requirement**
A – Task Organization	National Imagery Collection and Analysis
B– Intelligence	Interagency Data Sharing (CIA/NSA/DIA)
C – Operations	Common Operating Picture Generation
K – C4	Satellite Communications/Wireless
Q – Health Services	CBRNE Detection and Processing

Table 1. CONPLAN2502-05 Communications Requirements

[59] CDRUSNORTHCOM, *USNORTHCOM CONPLAN 2501-05, Defense Support of Civil Authorities*, 11April 2006, i.

What is significant about this table is that it can act as a point of origin for the methodology of the CBP process, particularly when developing models to capture shortfalls. An expanded version of this table will be introduced in Chapter V.

IV. DEFENSE PLANNING PART II: DISCERNING NEEDS

A. THE BOGSAT

As briefly discussed in the introduction of this thesis, the BOGSAT, a Bunch of Guys Sitting Around the Table method, is evolving towards a more quantitative method. Though efforts have occurred to change this paradigm, namely by instituting threat-based planning during the Cold War period and introducing CBP post Cold War, the BOGSAT paradigm is hard to kill. It continues to emerge in most corners of government, including the DoD, especially pertaining to areas of homeland defense.

A book authored by Ernest Forman, Professor of Management Science at George Washington University, discusses the pitfalls of the BOGSAT process. Here he iterates that the BOGSAT is the most frequently-used decision method in use today. Further he states, "Even though there may be considerable preparation for a BOGSAT, including information-gathering, and detailed analyses (e.g., financial, marketing, technical, political, etc.,), there are numerous problems with this approach. According to Peter Beck, 'These sessions are often dominated by the leader and rarely facilitated. The leader sets the tone and is often not challenged. If the group starts down the wrong path they rarely look back.'…However, times are changing and many organizations have been abandoning the BOGSAT in favor of more capable methods."[60]

Forman continues to reveal the central problem of the BOGSAT as the cognitive limitations of the human brain. Competent decision making requires following these subsequent steps:[61]

1. Perfectly defining the problem
2. Knowing all relevant information
3. Identifying all criteria
4. Accurately weighting all the criteria according to his/her goals.
5. Accurately accessing each alternative on each criterion.
6. Accurately calculating and choosing the alternative with the highest value.

[60] Forman, 5.

[61] Ibid., 6.

Also, the BOGSAT require the following to be relevant process: "A BOGSAT discussion typically involves dozens of 'things', e.g., issues, alternatives, pros, cons, objectives, criteria, etc."[62] Simply, most humans are not trained and/or conditioned to follow this mental checklist to ensure their decision making is sound. When the decision process grows too complex or stressful, humans will default to using their gut instincts or migrate toward the comfort zone of their emotional biases. Often, as a built-in coping mechanism, humans will attempt to simplify or de-scope the problem in order to comprehend it or find a low hanging fruit solution to rectify the problem. This is problematic as this simplifying or de-scoping often indeed changes the nature of the problem itself. Therefore, when a solution is offered, it is the wrong solution for the wrong problem.

Another issue that is related to this phenomenon is a term called thin slicing. Thin slicing is a method to make decisions quickly in times of crisis. Thin slicing is a technique that resides in the military and first-responder culture, where fireman, police, and soldiers, will make split decisions based on a sixth sense which is developed after years of exposure to life threatening situations where certain sounds, smells, or images prompt a person to decide or act quickly to save lives or thwart disaster.[63] Though this is a crucial skill for first responders, it could prove disastrous in the defense planning sector, as procuring capabilities requires methodical and careful planning where programs are funded over three, five year defense programs.

What is ironic about the defense culture is that the key decision-makers concerning capability procurement are flag officers who are typically force application operators who have developed the thin slicing technique in combat and major combat operations over years of military service. This would imply that these decision makers might be predisposed to thin slicing and come to the table ready to make split or gut reactions without following a methodology or type of model.

Perhaps this is why there is such opposition to defense planning processes that are steeped in rigor, such as CBP. It is a process that is foreign to the tactical culture.

[62] Forman, 5

[63] Malcolm Gladwell, *Blink: The Power of Thinking Without Thinking*, New York, NY: Time Warner Book Company, 2005.

Though flag officers have years of strategic and operational experience, their formative years were spent at the tactical level, relying on their gut and acting quickly in times of stress and crisis.

With regards to defense planning at USNORTHCOM, CBP has been adopted, but not fully embraced. In addition to JCIDS, NORTHCOM has developed a process called the Capabilities Review and Resource Assessment (CRRA). This is not to be associated with the CRRA used by the Air Force, which is the Capability Risk and Review Assessment. NORTHCOM's CRRA is conducted by J81 and is consistent with the JCIDS process. Though NORTHCOM is working to institute their version of the CRAA, capability decisions are still sometimes conducted using the BOGSAT method. This is not a problem unique to NORTHCOM. CBP is a new discipline within the DoD and will take years to modify a culture that cut its teeth on Cold War programmatics.

The same problems that perpetuate the BOGSAT at the senior decision making level is also felt at the action officer level of many staffs. Unlike the flag officer, who has had years of operational and strategic level exposure, the action officer may have little, if any, strategic experience. They come from the tactical arena where decisions are made quickly and they bring with them thin slicing skills that are razor sharp. This is also true for Program Element Managers (PEMs). PEMs think in terms of platforms and systems, not capabilities. Moreover, PEMs live in a culture where defending platforms occurs at all costs. The outcome of their fitness reports is directly proportional to the survival of their responsible system, not by the desired effect their systems provides to the combatant commander.

Another irony that exists on many staffs is that the director was once a PEM when he or she was a new field grade officer reporting to their first assignment at the Pentagon or Joint Staff. This makes for an interesting dynamic as staffs have essentially evolved, or are evolving, in a PEM culture. This is where the double-edged sword emerges. Services must defend programs that are directly tied to their portion of the total obligation(al) authority of the defense budget, while justifying the necessity of these programs that should be tied to its capability which, in-turn, produces a desired effect.

B. THREAT-BASED PLANNING AND OTHER CONCEPTUAL FRAMEWORKS

One way the DoD attempted to overcome the culture of the BOGSAT was to adopt a method of defense planning called threat-based planning. Threat-based planning provided utility during the Cold War when assessing the capability of a major adversary such as the Soviet Union. This method of planning works well with a peer competitor via the lens of a bi-polar international system. The bi-polar system provides a fair amount of stability to project threats and vulnerabilities for reasonably long periods of time. This system perpetuates technological advances which inherently become part of national infrastructures that directly effect economies and defense budgets. In reality, the Cold War and the era of threat-based planning ushered in a technological warfare culture where America deeply depended on technological advances to minimize vulnerabilities with the Soviets.

In addition to discerning threat, this form of planning also focuses on vulnerabilities which are requisite to a quantitative method adopted by McNamara during the Vietnam period. Threat-based planning also introduces scenarios as a way to provide context to overcome the vagueness associated with a pure numerical analysis. This methodology becomes a push-pull relationship, gauging threat and vulnerability which will ultimately prompt a requirement to rectify the perceived vulnerability. Requirements drive programs, which then drive production and procurement of hardware and systems.

The key problem with this method of planning was that it is a reactive process, matching tit for tat with the Soviets as they introduced new weapons into their arsenal. New weapons implied a new, or more, vulnerability which prompted a requirement to resolve that vulnerability with a new weapon or platform to deliver it. This phenomenon initiated the arms race which glutted America and Russia with enormous stock piles of troops and equipment providing, Americans with a false sense of national security. What threat-based planning really failed to accomplish was to measure the likelihood or intentions of the Soviets. This likelihood can be translated into risk, which this method of planning failed to determine. This process has the ability to send a nation down the wrong rabbit hole, completely procuring the wrong systems to minimize risk.

Other frameworks have been utilized over the years in addition to threat-based Planning. Some of these include: Top-Down Planning, Bottom-up Planning, Scenario Based Planning, Hedging, Technology, Fiscal, and Core Competencies, Capabilities and Missions Planning. Each has their strengths and weaknesses and collectively, have led to the evolvement of defense planning.

Top-Down Planning focuses on America's Grand and Defense Strategies and is very hierarchal by nature. Its strength is that it helps planners think in terms of ends with an emphasis on supporting national power such as: economic, political, and military relationships. However, it is too overarching by nature and the details of capabilities are often lost or hard to match to national objectives.[64]

Bottom-up Planning looks at improving existing capabilities with regards to current operational issues. Its advantage is that it is focuses on real world issues and is easy to conceptualize. Its shortfall is that it is nearsighted approach and fails to capture emerging threats and big picture issues.[65]

Scenario Based Planning is situationally driven, grounded by specific crises or major conflict operations. Like the bottom-up method, this planning is tangible and easy to conceptualize, often with clear priorities and objective defined. The greatest pitfall of this model is that the scenarios are illustrative, not predictive, often relying on old crises or engagements.[66]

Hedging is a method which focuses fully preparing or over preparing of any conceivable military tasking. It is effective as it captures the detail required to negate a myriad of threats, but is unrealistic as it is the most costly method available.[67]

Technology Planning, as the name implies, leverages technology to provide advantage over the adversary. The atomic bomb, space assets, and precision guided

---

[64] Henry C. Bartlett, G.Paul Holman, Jr. and Timothy E. Somes, *The Art of Strategy and Force Planning*, New Port, RI: Naval War College Press, 2005, 24-25.

[65] Ibid., 25.

[66] Ibid., 27.

[67] Ibid., 30.

munitions are examples of this type of planning. While the advantages are obvious, its shortfall is it often neglects non-material solutions as a way to optimize tactics, techniques, and procedures.[68]

The fiscal approach obviously uses the budget to drive this model. In reality, every planning meeting at the Pentagon has its roots tied to this process. While this process is effective for exercising fiscal discipline, it is difficult for this process to be tied to changes in threat or capability. For example, if 25% was shaved from a particular program, this does not necessarily mean that 25% of the systems capability is lost. Further, this same 25% cut to a program does not translate into a 25% increase in threat.

Finally, Core Competencies, Capabilities and Missions Planning is the newest predecessor to capabilities based planning. It incorporates many of the processes of the before mentioned models with the added nuance of mission planning. While this model is quite encompassing and realistic, it is too tactical in nature, focusing on the minutia of particular service missions, also missing the big picture of national strategy.

It is apparent with the introduction of these various models, that defense planning is a challenging art and not necessarily a science. These models led the way to capability-based planning, particularly the JCIDS process adopted by the DoD. Each model introduced at the Pentagon brought with it the hope that the DoD was closer to a solution to better manage programs and risk. It is also worthy to note that with each silver bullet introduced, a spirit of cynicism continued to grow amongst the senior civil servants who in disgust resorted back to their comfort zone, aka the BOGSAT, abandoning rigorized methodologies.

Many contend that capability-based planning is nothing new, but merely a hodgepodge of failed models cobbled together to satisfy the findings of the 2001 Quadrennial Defense Review (QDR). Regardless, this new model has become the central theme of defense planning and is more than likely here to stay until the QDR deems an adequate replacement.

---

[68] Henry C. Bartlett, G.Paul Holman, Jr. and Timothy E. Somes, *The Art of Strategy and Force Planning*, New Port, RI: Naval War College Press, 2005, 24-25.

The DoD and services have adopted it and continue to refine its processes, while planners grapple with the intricacies of this paradigm know as capability-based planning.

C. JCIDS

As discussed in the previous and introduction sections of this thesis, JCIDS is the current model used by the DoD to capture capabilities strengths and gaps to help shape funding decisions for a wide variety disciplines or focus areas, such as: force protection, battlespace awareness, force application, focused logistics, command and control, and the network-centric environment. These disciplines are encapsulated by what is known as a family of Joint Operations Concepts. The following statement captures the intent of this design: "In April 2003, the Secretary of Defense directed the development of the Joint Operations Concepts (JOpsC) family. This family consists of a Capstone Concept for Joint Operations (CCJO), Joint Operating Concepts (JOCs), Joint Functional Concepts (JFCs), and Joint Integrating Concepts (JICs). These concepts look beyond the FYDP out to 20 years."[69]

Each concept has its place in the CBP process and each concept is published in corresponding documents. The following definitions and figure help delineate this family of documents:

- **CCJO** - "Overarching concept of the JOpsC family that guides development of future joint force capabilities. Broadly describes how the joint force is expected to operate in the mid to far term, reflects enduring national interests derived from strategic guidance, and identifies the key characteristics of the Future Joint Force."[70]
- **JOC** - **"**Operational-level descriptions of how a Joint Force Commander will accomplish a strategic mission through the conduct of operational-level military operations within a campaign. Applies the CCJO solution and joint force characteristics to a more specific military problem. Identifies challenges, key ideas for solving those challenges, effects to be

[69] The Chairmen of the Joint Chiefs of Staff, *JOpsC Family of Joint Concepts - Executive Summaries,* 23 August 2005, 3.

[70] Ibid., 5.

generated to achieve objectives, essential capabilities likely needed to achieve objectives and the relevant conditions in which the capabilities must be applied."[71]

- **JFC** - "Describes how the Future Joint Force will perform a particular military function across the full ROMO. JFCs apply the CCJO solution and joint force characteristics to the specific military problem. They identify the required functional capabilities needed to generate the effects identified in JOCs and identify attributes needed to functionally support the Future Joint Force. JFCs address Tier 1 Level Joint Capability Areas."[72]

- **JIC** - "Describe how a Joint Force Commander will perform his operations or functions that are a subset of JOC and JFC capabilities. JICs address Tier 2 Level or below Joint Capability Areas. JICs have the narrowest focus of all Joint Future Concepts and describe capabilities and decompose them into task level detail. An illustrative vignette is applied to the JIC to describe the environment in which these tasks will be performed. The standard of performance for these tasks is described in a common taxonomy for concepts and capabilities."[73]

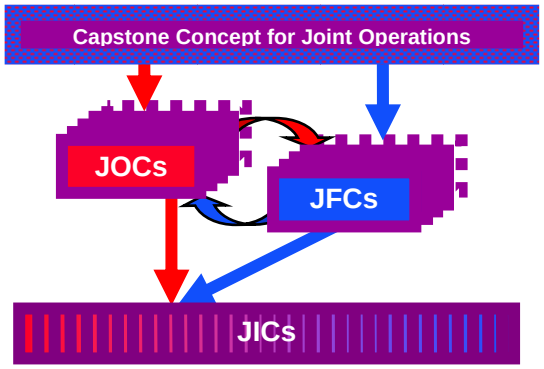

Figure 1. JOpsC Family[74]

[71] The Chairmen of the Joint Chiefs of Staff, *JOpsC Family of Joint Concepts - Executive Summaries,* 23 August 2005, 6.

[72] Ibid., 11.

[73] Ibid., 20.

[74] Ibid., 4.

This family of documents thus becomes the reference materials for Capability-Based Assessments (CBA) within the JCIDS process. First it is important to understand what the CBA is. CJCSI 3170.01F, states: "The CBA is the JCIDS analysis process that includes three phases: the FAA [functional area analysis], the FNA [functional needs analysis], and the FSA [functional solutions analysis]."[75]

The FAA defines the military problem, scopes the problem, introduces capabilities needed, and links those capabilities to defense strategy. The FNA is the portion of the CBA that begins to discern gaps in capabilities. Here capabilities are scored using the context of the scenario in the FAA. The FSA, as the name implies, is the process which recommends solutions to capability gaps ascertained in the FNA. These solutions are often broad and overarching, identifying both material and non-materials solutions to rectify the gaps.

Therefore, for the purposes of this thesis, analysis of the Net-Centric Environment JFC and JIC will be conducted as the JFC and JIC contain the specified parameters to conduct the CBA such, as: the scenario or vignette and the capabilities and attributes to be scored during the assessment to determine gaps or excess. The following figure helps visualize this complex process:

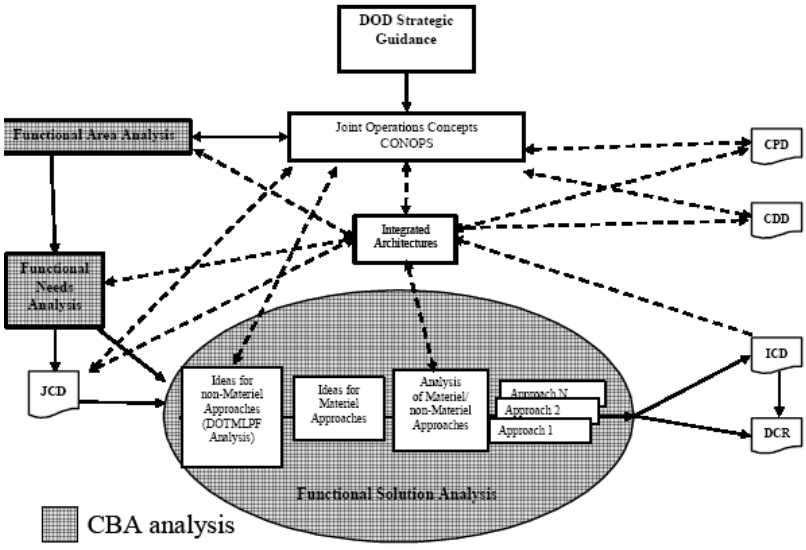

Figure 2. The JCIDS Analysis Process[76]

[75] The Chairmen of the Joint Chiefs of Staff, *Capabilities-Based Assessment User's Guide*, December 2006, 4.

[76] Ibid., 6.

THIS PAGE INTENTIONALLY LEFT BLANK

V. IDENTIFYING COMMUNICATION SHORTFALLS FOR USNORTHCOM

A. CURRENT METHODOLOGY

NORTHCOM has adopted a derivative of JCIDS called the CRAA. This CRRA is not be confused with the Air Force CRRA, but is essentially JCIDS coupled with an Interagency Coordination (IC) component to facilitate their mission of providing defense support for civil authorities. This IC component allows collaboration with interagency partners which, in-turn, provides input for their CRRA process.

The CRRA is conducted annually by the J5 and J8, with J8 acting as office of primary responsibility for the overall codification process. The CRRA work in concert with the planning, programming, budgeting, and execution cycle, to support NORAD and NORTHCOM's commitment to fulfill national military strategy. This methodology is used to help identify current and future capabilities and help guide the command's investment decisions. The output of this process is presented to the Office of Secretary of Defense, other defense agencies, the Joint Staff, the services, and to the Canadian department of National Defense to inform this community on capability development, acquisition, sustainment, and investment needs.[77]

Guidance for the CRRA process is contained in NORAD/USNORTHCOM Instruction 90-144 and is compliant with the following DoD and Joint instructions/processes:

- CJCS Instruction 3170.01E, JCIDS
- CJCS Instruction 6212.01D, Interoperability and Supportability of Information Technology and National Security Systems
- DoD Directive 5000.1, the Defense Acquisition System
- DoD Instruction 5000.2, Operation of the Defense Acquisition System
- DoD Directive 7045.7, Implementation of the Planning, Programming, Budgeting System

[77] NORAD/USNORTHCOM Instruction 90-144, *Capabilities Review and Resource Assessment*, 1 November 2006, 2-3.

As the CRRA is a new process, it is more of a vision than a reality. This is the first time the CRRA has been conducted and, as with any new concept, it is just beginning to make traction. NORTHCOM is the newest combatant command and is barely getting its arms around JCIDS, let alone its recent cousin, the CRRA. Though it offers promise, particularly regarding its interagency collaboration piece, it will have to survive cultural barriers and the plethora of taskings that seem to plague higher headquarters organizations.

As for determining communications shortfalls for homeland defense, the J6 has yet to adopt the CRRA. Currently, they are utilizing the JCIDS process, primarily focusing on the NCE JFC and JIC as the instruments to conduct their analysis. Though this directorate is valiant in pursuing this process, the NCE JFC and JIC are laden with their own unique set of problems which impede the NCE planning process in the context of homeland defense and security.

This leads to the most important aspect of capability-based planning: the context in which one discerns capability gaps. The context is based on the scenario that is at the front end of the model. This is the lens that helps the planners and subject matter experts determine what environment they are to operate within. In the case of JCIDS or NORTHCOM's CRRA, this scenario is contained in the JFC. The scenario contained in the NCE JFC is a vignette occurring in Turkey, involving the capital city which is struck by an 8.2 magnitude earthquake, displacing thousands of Turkish citizens and destroying or disrupting Turkey's critical infrastructure.[78] While this type of vignette is likely to occur, much like how Hurricane Katrina transpired, it is only a single event. Though it is an adequate starting point, NORTHCOM will surely be faced with multiple events that will exceed the intensity of a natural disaster.

More appropriately, the NCE JFC should contain a series of events that would reside in NORTHCOM's purview. More precisely, multiple events in the homeland and abroad are more realistic. Events such as a dirty bomb detonation in the port of Long Beach, followed by a Tsunami in Australia, topped off by a string of IEDs in downtown

[78] Joint Functional Concept, *Net-Centric Environment*, 4.

Manhattan during rush hour. The diversity and intensity of these simultaneous events would provide the adequate stress in the model to keep SMEs and planners attentive.

B. STRENGTHS AND WEAKNESSES OF CURRENT PROCESSES

In the previous section, a key weakness was identified that now begins to clear the path for what is right and what is wrong with NORTHCOM's model. Starting with its strengths was the fact that the J8 Directorate realized JCIDS was a not one-size fits all model. Their initiative to establish the CRRA is evidence that the command is serious about solving interagency NCE shortfalls. Establishing the IC component of the CRRA is a very pragmatic solution to enable collaboration with non-DoD partners. While this is often a painful pursuit of clashing cultures, it will pay dividends when capturing the right expertise and perspectives when pinned together during reoccurring forums. Eventually, these forums will condition themselves to overcome these cultural barriers, ultimately developing the right network of planners to solve interoperability problems.[79]

Further, the CRRA provides NORTHCOM with a quantitative assessment of end-to-end look at capabilities, addressing desired effects. It attempts to link strategy to capabilities and then, to desired effects. This process is the catalyst to evolve from the BOGSAT which still resides at NORTHCOM and other higher headquarter institutions.[80]

While the J8 is working hard to institutionalize a capability-based model that works for the command, several weaknesses are inherent in the process. These weaknesses apply to both the JCIDS and CRRA models adopted by NORTHCOM. This implies that NORTHCOM is not solely in error, but that the Joint Staff has created a model that is too complex and labor intensive. In an effort to design an encompassing process, it is has become over engineered and far too difficult to comprehend. Too many working parts reside in the process and it requires months, if not years to master. Over 500 pages of esoteric guidance must be consumed before a participant is to gain an elementary working knowledge of the NCE portion of JCIDS.

---

[79] Brian Byrne, Program Analyst, Programs, Resources, and Analysis Directorate, NORAD/USNORTHCOM, N-NC/J81, Interview by Kevin Wilson, (2007).

[80] Ibid.

Action officers assigned to labor in this discipline lack the continuity to gain in depth expertise. Often, action officers change assignments several times within their tours, barely scratching the surface, then moving on to new duties. Even if the directorate is staffed with an action officer who can provide continuity, the SMEs tasked to provide the analysis have to be trained or retrained to perform their duties, often in a very narrow time slot. What exacerbates this problem further is the fact that few action officers are dedicated solely to the JCIDS or CRRA process. They are encumbered with multiple taskings unrelated to capability-based planning, that clouds their ability to focus and spend the adequate time necessary to develop the proper methodology and analysis to garner NCE gaps.

The same problems experienced by the action officers responsible to administer these processes also pertain to the SMEs who are tasked to perform the scoring and analysis of the JFCs and JICs. Few, if any, headquarters possess the sufficient number of SMEs organically to analyze the diversity and complexity of the NCE JFC and JIC. Thus, headquarters must solicit help throughout the services to find the right mixture of expertise to conduct the appropriate level of analysis needed. Hence, the problems of over tasking and lack of continuity permeates into this body, where understanding and ample time to dedicate to the process is absent. This ultimately affects the control group used, as the base of action officers and SMEs are so dynamic that perceptions, expertise, and interest drive different scores and outcomes from year to year. Just finding and maintaining a usable repository of SME who are willing in able to participate in the planning process, is a full time responsibility.

In addition to personnel issues that affect the control group, the ability to quantify the criterion of the NCE standards and measures of the JIC is problematic. This criterion is too specific to be scored in any given scenario. For example, if response time to provide connection to US and non-US networks is the standard being measured and the criteria is 30-60 seconds, how can that be measured? Does someone have a stop watch to monitor every connection in every work center? Of course not. Thus this criterion loses its utility and SMEs typically respond with something like, 'it depends.'[81]

[81] Maria Grider, Branch Chief Future Capabilities, Plans, and Policy Division, NORAD/USNORTHCOM, N-NC/J65, Interview by Kevin Wilson, (2007).

Further, the amount of capabilities, tasks, and standards contained in the JIC are too great and require far too much time to analyze. Many of these can be eliminated to simplify and expedite the process. Most organizations lack the luxury for their action officers to dedicate this much effort in a supporting role.

C. AN OPTIMZIED PROPOSAL[82]

In an attempt to elevate the problems associated with the JCIDS model, this thesis offers a more intuitive and simplified capability-based model. The model offered here is an overview of a hybrid of several planning models, not an all encompassing proposal, but contains sufficient detail to articulate its utility. For the purposes of this model the following critical elements must be covered: the Scenario, the Master Capabilities Library (MCL), SME Selection, and the Forum.

The Scenario

The scenario is the first lens to look through and the most important. The scenario is the event or events which provides context or sets the stage of the operation. It provides the who, what, when, where, and why of the operation. For example, if the military is engaged in operations with civil authorities, such as evacuation efforts due to natural disaster or a CBRNE event, the scenario helps provide the operational environment or situation in which personnel and equipment operate. This is critical as it helps planners visualize what stressors affect the operation.

For the intent of this model, it is important to select a scenario that is most stressing. This ensures planners select the right capabilities to be evaluated or applied to the event. The Office of Secretary of Defense (OSD) has been tasked to identify the most stressing scenarios to our nation and military. Two Major Conflict Operations (MCOs) are applied, plus four vignettes should be applied to the methodology.[83] Vignettes are CBRNE and natural disaster events and thus are perfectly matched for first-responder

[82] This methodology was my design while I was assigned to the Air Force Concept of Operations, AF/A5XC-SC, Pentagon, Washington, D.C. It was validated by the Air Force Communications Agency, Air Mobility Command, A3 & A6, Scott AFB, IL. The data derived from this methodology was published in the 2006 Air Force Capabilities Risk and Review Assessment and in Air Force Planning and Program Guidance. The NCE CBP methodology I propose is a tailored version of my original work to be used by USNORTHCOM to identify first-responder NCE shortfalls.

[83] CBAM 101 Training, AF/A5XC-SC, Colonel David Johnson, USAF. (2006).

operations. Further, a CBRNE event would be the most stressing to civil authority and first-responder communication systems, as it is a worst case scenario which could occur to our country. Communications systems would have to be survivable to electro magnetic pulse, interoperable with military, federal, state, and local agencies. This does not imply that capabilities must be gold plated, but acts as a reminder of the severe environment present for planners and SME to keep in the back of their minds when conducting analysis. In order to facilitate this, a scripted briefing containing the details of the scenario and its vignettes must be crafted and presented to the entire body conducting the analysis at the initial stage of the process. Also, it should remain present during the duration of the planning session and be cited in the published findings of the analysis. This assists planners and SME from reverting to previous real world events or lessons learned which not the intent of this type of analysis.

The intent of this model is to capture current and future capability shortfalls for current plus two FYDPs, thus aligning itself with the POM of the services supporting NORTHCOM. If documented correctly, this provides extremely important justification to programmers to defend their systems that fill the shortfall gap. However, this must be validated by participants from the Joint Staff, NORHCOM, and the services.

The MCL

The MCL is a repository of capabilities, not tasks. The MCL consists of five distinct parts: the category, the domain, the capability, the attribute, and the Measure of Performance (MOP). It is the primary tools for SMEs to score the maturity of capabilities

The category, Provide the Network-Centric Environment, is a modified definition from the NCE JFC which is more applicable for HLD operations. It should read: Connectivity and interoperability that allows all DoD users and mission partners to include: Joint, Coalition, Inter-Agency, Federal, State, and Local First Responder users to share information when they need it in a form they can understand and act on it with confidence, and protects information from those who should not have it.

The domain is the environment personnel and equipment operates in, such as: land, sea, air, and space. The domains are defined in the following manner.

- Land – Operations where personnel and equipment reside on the ground, such as: search and rescue operations, police and fire operations, Command and Control (C2), Nuclear C2 (NC3), and Special Operations (SOF) missions.
- Sea – Operations where personnel and equipment reside on the water, ocean, lake, and river, such as: port security, search and rescue, counter sea operations, and NC3.
- Air – Operations where personnel and equipment reside in the air, such as: air strike, C2, Intelligence, Surveillance and Reconnaissance (ISR), and, NC3.
- Space - Provide services/connectivity to and from assets used in operations that occur in space, such as: space situational awareness, offensive counter space, defensive counter space, missile warning, surveillance, communications, precision navigation and timing, nuclear command and control, and weather.

As previously mentioned, the capability is what service is being delivered, not the system or the solution. Therefore NCE capabilities in its simplest form are: provide voice, video, or data services. Capabilities are defined in the following manner:

- Voice – Information, such as: radio, phone, interphone, voice over Internet Protocol, or public address system.
- Video – Information, such as: streaming video, video teleconferencing, live transmissions, or recorded video.
- Data – Information, such as: text or imagery, such as: digitized photos, forms, publications, email, messages, web pages, chat sessions, or audio files.

Attributes are the characteristics of the capability which gives it uniqueness or desired level of performance. These attributes are defined in the following manner:

- Timely - Expected timeliness to meet mission requirements. Implies latency, speed, and responsiveness of systems and information in all environments.
- Availability - Information access, anytime/anywhere. Implies adequate bandwidth, redundancy and self-healing/self-forming architecture. Includes Machine to Machine (M2M) interconnectivity.
- Survivable - Expected to survive in multi-environments: electro-magnetic pulse, directed energy attack, and radio frequency attack. Implies the capability is hardened to withstand physical attack.
- Low Probability of Intercept/Low Probability of Detect - Ability to provide low probability of intercept and detect. Implies ability to operate in anti-access environments where low observable and stealth are required towards mission success.
- Protected - Information is expected to withstand information attack or compromise from an adversary. Includes information assurance attributes, such as: authenticity and non-repudiation. Further implies multi-level security capabilities to appropriately share information with coalition, DoD, inter-agency, federal, state, and local partners.
- Useable - Ability to operate the system with little or no effort or training. Implies the system is intuitive to operate and the output is decision quality, discernable, and easy to comprehend. Further implies the appropriate human factor analysis has occurred to ensure ease of operation and comprehension of information flow.

The final component of the MCL is the MOP. The MOP is the value function that is scored by operators, planners, and technical experts to assess the respective capability and its attribute. The process consists of two parts: establishing the value function and assessing the capability and attribute. Establishing the value function is accomplished first. This is where the operator expresses the required level of performance and what attribute is essential for mission success. Then, NCE planners and Subject Matter Experts

(SME) will assess and score to determine if existing capabilities meet the value function. If not, then a potential capability gap is discerned and recorded for further analysis and validation.

Four categories are assigned to the value function: No Military Value (NMV), Limited Military Value (LMV), Good Enough (GE), and More Doesn't Matter (MDM). The critical step is establishing the GE value, as GE is the goal to discerning if appropriate capability exists. Anything less implies a capability shortfall, while anything more implies excess and the capability does nothing more to enhance the mission. This is accomplished in a collaborative effort with planners and operators looking through the scenario lens and judging what capabilities are needed, what corresponding attribute is essential, and what MOP is necessary to accomplish the mission.

The following table illustrates the useable attribute:

Useable	1. Unable: NMV: 1-10
Ability to operate the system with little or no effort or training. Implies the system is intuitive to operate and the output is decision quality, discernable, and easy to comprehend. Further implies the appropriate human factor analysis has occurred to ensure ease of operation and comprehension of information flow.	2. Extreme Difficulty: NMV: 11-20
	3. Considerable difficulty: LMV 21-40
	4. With Some Effort: LMV: 41-79
	5. With Minimal Effort: GE: 80
	6. Completely Intuitive: MDM: 81-100

Table 2. Attribute and MOP Depiction

For example, if an operator needed data services in the land domain, useable would be a relevant attribute. Now, at what level does useable become necessary to accomplish the mission? What threshold can the operator live with where more really does not matter to complete the mission? If completely intuitive provides no advantage over minimal effort, then the value function becomes 5- with minimal effort.

Once the value function has been set, now the planner and SME can assess to determine what systems and platforms provide this type of capability and perform at the level. If not, then a potential capability shortfall may exist.

To illustrate this collective process, consider if Monterey was responding to an earthquake. The earthquake would become the scenario or vignette and would contain certain stressors such as, no electrical power, buildings destroyed, fire, and etc. The first responder or fireman would have to determine what communication/NCE capability is needed to accomplish their mission. They decide handheld radios are necessary and useable is a required attribute. They further determine that the GE value is 5, useable with minimal effort. Now the SME and planner can assess their current radios to determine if it meets that value. If not, a possible shortfall exists and then they begin the validation process to discern if shortfalls exist and begin to package the data in a decision quality format. Once the data is validated and formatted, planners present the data to decision makers, who prioritize funding requirements for annual procurement budget decisions. This process provides an objective and quantitative approach.

SME Selection

Another critical element of this model is the selection of subject matter experts. As described in the MCL portion of this thesis, the MOP is a two sided equation, analyzed by two types of SMEs. The operational SME is an expert well-versed in a particular operation contained in the scenario. For the purposes of the HLD vignette discussed earlier where Monterey suffered from an earthquake, fireman, police, and military assisting in the disaster would quantify what is needed to establish the value function. Further, interagency partners, such as FEMA, DHS, and the Red Cross, must be present to state their needs. These groups of experts capture the communication requirements pertaining to that scenario.

The second set of SMEs is known as system experts well versed in capabilities these systems deliver. Typically these are programmers, engineers, and acquisition specialists who intimately know the characteristics of NCE equipment. These SMEs can match the capability of these systems to the value function set by the operational SMEs. Though the capability-based model is to be system agnostic, eventually matching must occur as systems ultimately provide capability. However, this model limits the cart

before the horse issue typically occurring in non-capability models, as the operator is present during the duration of the analysis, acting as an honest broker, constantly articulating operational need.

SME selection is often viewed as a lesser important duty of the process, but it requires meticulous record keeping to ensure SMEs are available and possess current and relevant knowledge. This requires reoccurring dialog between NORTHCOM, the SMEs, and their leadership to foster this network of personnel between planning cycles. This helps alleviate the cultural barriers in interagency forums, merely by conducting open and reoccurring chats to champion collective issues. This investment in social capital requires no formal design or procurement boards to establish. It is a simple exercise where leaders, SMEs, and planners pick up the phone or send an email to maintain contact and collectively work towards solving problems.

The Forum

An additional element of this process often overlooked is the type of forum used to capture perspective shortfalls. The JCIDS process is too formal and complex to facilitate a large interagency body. Often data calls are sent out beyond the confines of the headquarters without much facilitation, where SMEs and action officers remotely fill in spreadsheets within the walls of their cubicles. Hence a balance must occur where the forum is not too formal to stifle problem solving, but not too relaxed an atmosphere as the ad hock BOGSAT.

Initially, NORTHCOM should host the forum at their headquarters with a good facilitator to guide the process. Anything over a week in duration typically lacks productivity, as it will exceed human attention and interest span. The forum must be conducted in a true interagency fashion, with the right mixture of SMEs present from the respective agencies anticipated to participate in the given HLD/HLS scenario. The introductory session should include leadership from these agencies to champion the process and elicit support for it. After a few gatherings have been hosted at NORTHCOM, the forum could be rotated and hosted by one of the other interagency groups, further improving relationships and lowering cultural barriers.

The forum should be recorded to ensure the important sound bites have been captured and can be included in the findings of the planning session. Once the planning session is concluded by SMEs and planners, the packaged findings should be validated by the leadership of these various agencies. Again, this should be conducted in a collaborative setting, where collective buy in and consensus is achieved.

This could serve as a seamless interagency planning process, where these senior leaders would present their findings to the house and senate in a true collaborative manner. Obviously it is absurd to assume 100 percent agreement amongst these diverse groups, but a mere 50 percent solution would be a far cry better than the current process.

VI. CONCLUSION

A. SUMMARY OF FINDINGS AND RECOMMENDATIONS

As this thesis concludes, it must now readdress the initial research question: Does CBP possess the right methodology to assist defense planners and programmers in determining capability gaps/shortfalls? To assist in ascertaining this, the following sub-questions must be answered:

- *How can the CBP process be more intuitive?*

The obvious solution to this problem is to consider the audience who will review the data. In this application, the audience will be at the flag officer and senior executive service rank. This implies that the time constraints of this group are precious and the process must be immediately understood to garner their buy-in. Analytical rigor is important, but not to the extent that a primer in network or engineering fundamentals is necessary to understand the results.

This is why a graduated scale of 1-5 is recommended to measure the performance of the attributes in the network-centric master capabilities list. Measuring availability in megabits per second versus available when needed has very little meaning to a career fighter pilot or infantryman. As operational experts will determine the value function, or the good enough value, of the model, it must be expressed in consumer terms. For example, when a consumer is purchasing a high speed internet connection for their home or office, few consumers know they need a connection speed of 1.5 megabits per second. However, they realize the need for a connection that is available when needed, reliable, and responsive.

Further, the overall CBP model must not contain too many moving parts. The current JCIDS model involves three distinct phases: the functional area analysis, the functional needs analysis, and the function solutions analysis. These are conducted in a stove pipe fashion; coupled with the ambiguity of the JFC and JIC, it makes for a far too complex model. Therefore, the design must be seamless and conducted in the same forum by the same SMEs to the greatest extent possible.

- *How does CBP determine capability gaps?*

The capability-based model is a hybrid of past and existing defense planning models that have evolved over time. It integrates components of the scenario-based planning, hedging, technology, fiscal, core competencies, capabilities and missions planning, and threat-based models discussed in Chapter IV of this thesis. Therefore, if constructed and conducted properly, the CBP model offers the most innovative and exhaustive approach.

The ultimate advantage of capability-based planning is that it minimizes the BOGSAT phenomenon that resides in most military headquarters. CBP offers a model that has been vetted and scored by SMEs across many different disciplines from many different organizations. It reduces making decisions in a vacuum and eliminates the emotional factor of funding pet rock programs. It is a process steeped in capabilities, not tasks or systems, which produce a quantifiable correlation to the shortfall, regardless if using a capability library or JIC for scoring.

The use of the scenario as the initial lens provides context, which is the most important phase of this planning process. It offers situational vignettes which provide flexibility when forecasting threat or adversary capability in current and out year planning cycles. It helps operators dial in their requirements and articulate specific capability needs.

The establishing of value functions set by the operator helps determine the good enough unit of measure in order to accomplish mission requirements. This helps eliminate gold plating that engineers tend to be fond of as they fall in love with their respective designs and systems. This should help restrain cost overruns and identify duplicate capabilities or areas that do not provide military value or utility.

What is useful regarding the proposed methodology, specifically addressing the master capability library, is in utilizing the four domains, i.e. air, land, sea, and space. This will call on experts from all branches of the service and interagency partners from the coast Guard, NRO, NSA, and NGA. This model will aid in the facilitating of joint and interagency collaboration and dialog.

- *How does the output of CBP provide meaningful data for decision makers to prioritize procurement funds? What is this data?*

CBP offers data that connects the dots between operator requirements, existing system capability, and what systems can bridge the shortfall gaps. It can aid in championing the utility of a system or it can provide quantifiable data that may justify program cancellation. For example, if a particular radio system is being developed and programmed, but it cannot be tied to an existing capability or future capability gap, decision makers should question its utility and may desire to divert funds to programs that indeed can be traced to urgent capability needs.

Regarding the data types that may be useful to decision makers, this is dependent again on the audience or background of the principals making fiscal decisions. Typically, operators prefer a variation of a stoplight chart that appeals to their thin slicing culture. The following chart could act as template for output data for decision makers.

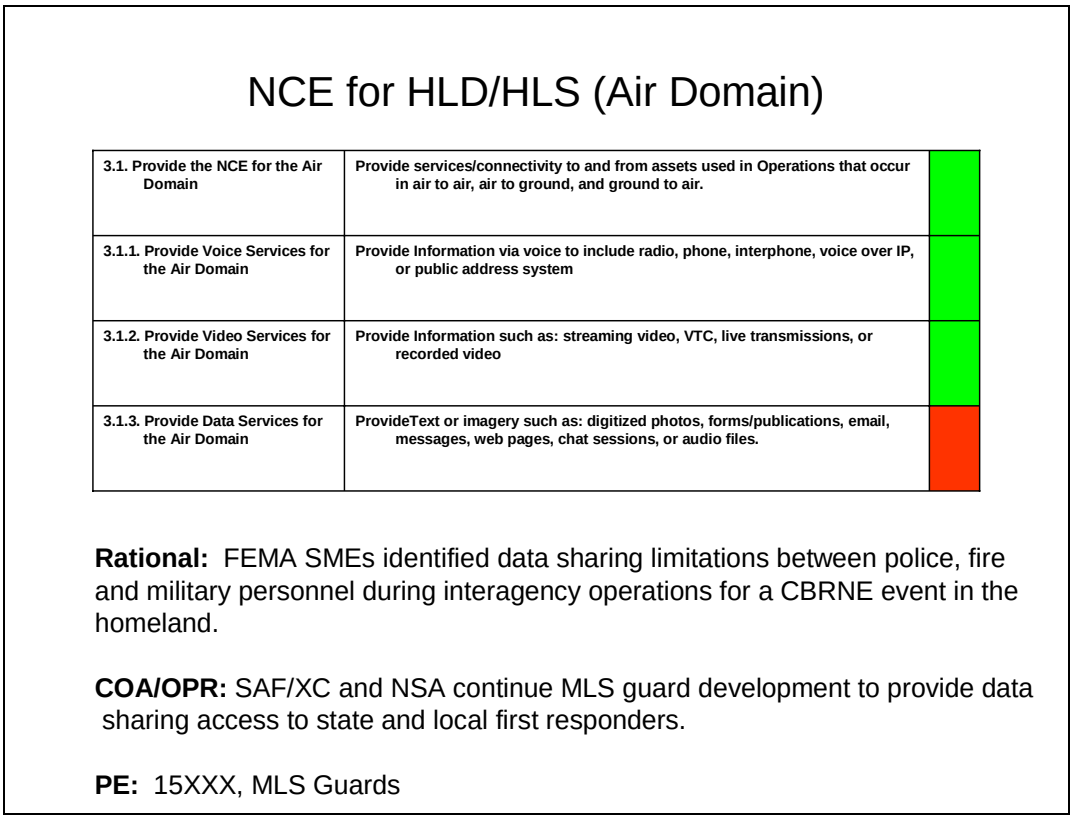

Figure 3. CBP Data Output Example

- *How can CBP be improved to better determine communication shortfalls?*

In addition to making the model and process more intuitive across a wide body of operator and system SMEs, the measures of performance must be quantifiable and the justification of the score must be captured. Eliminating the complexity of the process, i.e. migrating to an MCL versus the JFC and JIC, would expedite the data collection processes considerable. It is well understood that planners desire a comprehensive model to ensure no stone is un-turned. However, the over engineering of the JCIDS process produces too much overhead and time spent to complete the planning process. In times of crisis, where SMEs are dragged out of their operational environment to participate in the CBP process, time and talent management is critical. Thus, a balance must be achieved to provide a reasonably feasible methodology that eliminates the ambiguity and time restraints associated with JCIDS.

This leads the discussion back to the overarching question of this thesis, which is: Does CBP possess the right methodology for defense planners and programmers in determining capability gaps/shortfalls? The emphatic answer is, if JCIDS is the approach used, no. JCIDs must be transformed to a simpler and more intuitive process. However, regardless of the methodology adopted, failure to conduct the planning session in an interagency environment will continue to provide myopic outcomes, with stovepipe solutions feebly provided to fill these gaps.

This research problem is inherently an interagency problem. Therefore, the problem solving must occur in an interagency environment. Defense planning cannot continue to function in a vacuum. Cultural barriers must be leveled and this may be best motivated by controlling the purse strings. Interoperability standards should be designed into the planning, programming, and acquisition process. Interoperable engineering standards can then be validated before programs progress, ultimately being coordinated before an interagency working group.

This working group could participate in House and Senate appropriations committees to ensure the collective need is articulated and championed. Realistically then, for the culture to change via the stick of controlling the purse strings, congressional directives and oversight must occur to facilitate this change. Perhaps a derivative of the

Nichols/Goldwater Act might be the instrument to force reform of the defense planning process. This initiative might eventually change the course of this bureaucratic and inefficient discipline.

In addition to legislative measures, a heightened awareness of the capability-based planning process must propagate within the DoD and its interagency partners. This may be facilitated by incorporating a training module in existing curriculums for action officers prior to starting their staff assignment. Further, reoccurring training could include a module of refresher training that could be implemented as an annual requirement. Familiarity training should also be made available to SMEs upon their selection to participate in a CBP forum. This could be a web-based module completed prior to their participation in a CBP forum.

Perhaps more effective than familiarity training is a certification course, much like that which is encouraged for the acquisition community. This could act as an incentive for career planners and programmers to enhance their marketability and promotion opportunities. Further emphasis should be introduced into professional military education environments, such as: command staff and war colleges and civilian fellowship education programs.

One final recommendation of the overall CBP process would be to focus on non-material solutions to fill capability gaps. Though it is implied, too much emphasis is placed on matching systems to fill these gaps. Ample time must be spent on the entire DOTMLPF spectrum as a way to fill capability gaps. The obvious reason of why this fails to occur is that non-material solutions are less glamorous. Frankly, material solutions produce the most revenue and are more tangible to discuss and plan for. Optimizing business practices, which are normally tied to non-material solutions, should be the first area of house cleaning. However, in times of extraordinarily lucrative defense contracts, non-material solutions lose their luster.

B. WHO NEEDS IT?

Since capabilities are ultimately tied to programs and fiscal expenditures, CBP has its tentacles embedded into many organizations within the DoD. Currently the

acquisition community, J5 and J8 embraces CBP, but other organizations have been slow to follow suit. Regarding communication and NCE gap analysis, J6 directorates across the DoD would benefit greatly if all were on the same sheet of music to adopt a standardized methodology. It is also imperative that these three directorates establish a more cohesive environment during the planning process. It is always disenchanting to discover that so few action officers have coordinated on NCE gap analysis across a headquarters organization. Every Power Point slide or talking paper must be reintroduced and explained *ad nauseum* for it to move up the bureaucratic ladder. Ironically, it is the financial management and comptroller community which understands CBP the least. While they are well versed at moving different pots of money around within the TOA, they seem less concerned about how the fiscal decision was reached to do so.

Ultimately, the entire J staff should be in lock step regarding CBP. Since NCE is such an enabling capability, every directorate is touched by its capability. Though the J5, J6, and J8 are the directorates responsible for conducting the process, the J1, J2, J3, and J4 are the primary stake holders and ultimate recipients of NCE capabilities.

In addition to headquarter organizations, center and agencies within the DoD could benefit greatly from the CBP model. First and foremost would be DISA. As DISA is DoD's executive agent for communications and NCE, DISA may provide SME support and senior leader oversight. The National Reconnaissance Office (NRO) is another obvious choice of an organization that could gain from the CBP experience. As dissemination of intelligence information obtained from the various space and sensor platforms, the NRO is critical to the defense of the nation and their participation and advocacy in the CBP process is key. Ideally, NORTHCOM, DISA, the NRO, and DHS could form the nucleus to champion communication shortfall analysis for homeland defense. This collaborative model could be optimized over time, eliminating barriers and fostering effective relationships to solve this interagency problem.

LIST OF REFERENCES

Air Force Instruction 10-604. *Capability-Based Planning*. Washington DC: 2006.

Air Force Master Capabilities Library, version 6.0, Washington DC: 2007.

Bartlett, Henry C., Holman, Paul G Jr., and Somes, Timothy E. "*The Art of Strategy and Force Planning."* New Port, RI: Naval War College Press, 2005.

Byrne, Brian, Program Analyst, Programs, Resources, and Analysis Directorate, NORAD/USNORTHCOM, N-NC/J81, Interview by Kevin Wilson, (2007).

CDRUSNORTHCOM. USNORTHCOM CONPLAN 2502-05, *Defense Support of Civil Authorities*. Colorado Springs, CO: April 2006.

Chairman of the Joint Chiefs of Staff, *Capabilities-Based Assessment User's Guide.* Washington DC: December 2006.

Chairman of the Joint Chiefs Instruction 3170.01C. *Joint Capabilities Integration and Development System*. Washington DC: 2003.

Chairman of the Joint Chiefs of Staff Joint Functional Concept. *Battle Space Awareness*. Washington DC: 2003.

Chairman of the Joint Chiefs of Staff Joint Functional Concept. *Joint Command and Control*. Washington DC: 2005.

Chairman of the Joint Chiefs of Staff Joint Functional Concept. *Net-Centric Environment*. Washington DC: 2005.

Chairman of the Joint Chiefs of Staff. *JOpsC Family of Joint Concepts – Executive Summaries*. Washington DC: 2005.

Chairman of the Joint Chief of Staff Manual 3170.01B, *Operation of the Joint Capabilities Integration and Development System.* Washington DC: 11 May 2005).

Chairman of the Joint Chief of Staff Manual 3170.01B, *Operation of the Joint Capabilities Integration and Development System.* Washington DC: 11 May 2005).

Chairman of the Joint Chiefs of Staff, *Joint Capability Areas 101*, J7/JETCD. Washington DC: April 2007.

Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America: A Vision for Tomorrow.* Washington DC: 2004.

Committee on Evolution of Untethered Communications, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications National Research Council, *The Evolution of Untethered Communications*, National Academy Press: Washington, DC: 1997.

Combined Communications-Electronics Board, Authority for all Allied Communications Publication 167, *Glossary of Communications-Electronics Terms*, March 2005.

Connelly, Mike, Lieutenant Colonel, USAF, Deputy Director, Space and C4ISR Concept of Operations, AF/A5XC-SC, Pentagon, Washington, DC. Telephone Interview by Kevin Wilson on NORTHCOM's Capability-Based Planning Methodology by Kevin Wilson. Nov. 2006.

The Defense Information Agency, *FY 2004/2005 Budget Estimate*, Research, Development, Test, and Engineering Budget Item Justifications, February 2003.

The Department of Defense, *Strategy for Homeland Defense and Civil Support*, June 2005.

The Department of Defense, *The National Defense Strategy of the United States of America*. Washington DC: March 2005.

Forman, Ernest. "*Decision by Objectives: How to Convince Others that you are Right*." http://mdm.gwu.edu/forman/DBO.pdf. (Accessed 5 April 2007).

Gladwell, Malcolm. "Blink: the Power of Thinking Without Thinking. New York, NY. Time Warner Book Company: 2005.

Grider, Maria, Branch Chief Future Capabilities, Plans, and Policy Division, NORAD/USNORTHCOM, N-NC/J65, Interview by Kevin Wilson, (2007).

Johnson, David, Colonel. "CBAM 101." Communications FAT Pre-brief. Washington. 2006.

Naval Network Warfare Command. "FORCEnet." http://forcenet.navy.mil/fn-definition.htm (19 November 2006).

NORAD/USNORTHCOM. *Instruction 90-144, Capabilities Review and Resource Assessment*. Colorado Springs, CO: November 2006.

NORAD/USNORTHCOM. *Strategic Guidance – Defending Our Homeland*. Colorado Springs, CO: December 2006.

Schill, Ron, Ph.D., Visiting Professor, Monterey Institute of International Studies. Personal Interview by Kevin Wilson on Capability-Based Planning in the Corporate Sector. Pebble Beach. December 2006.

Secretary of Defense Memo. *Definition of Joint Capability Areas*. Washington DC: 6 May 2005.

U.S. Air Force Fact Sheet, *Defense System Communication Satellite*. http://www.af.mil/factsheets/factsheet_print.asp?fsID=95&page=1 (Accessed 5 April 2007).

U.S. Air Force Fact Sheet, *Defense Support Program Satellite*. http://www.af.mil/factsheets/factsheet.asp?id=96 (Accessed 5 April 2007).

The White House. *The National Security Strategy of the United States of America*. Washington DC: March 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Joints Chiefs of Staff
   J5, Strategic Plans and Policy
   Washington, D.C.

4. Joints Chiefs of Staff
   J6, Command, Control, Communications, and Computer Systems
   Washington, D.C.

5. Joints Chiefs of Staff
   J7, Operational Plans and Joint Force Development
   Washington, D.C.

6. NORAD - USNORTHCOM
   J6, Architectures and Integration Directorate
   Peterson Air Force Base, Colorado

7. NORAD - USNORTHCOM
   J8, Programs, Resources, and Analysis Directorate
   Peterson Air Force Base, Colorado

8. Headquarters United State Air Force
   AF/A5X, CONOPS Division
   Washington, D.C